Cybernance Corporation
Response to NIST Request for Information

CYBERNANCE
First In Cybergovernance

The following comments are based on our experience in studying, using, and adapting the Framework over the past 2 years. Although our company (Cybernance.com) was formed in February 2015, our founders are intimately familiar with the CSF though prior experience in research and consulting.

Our mission has been to translate the Framework into software, so that it may be more easily absorbed into companies who desire greater insight into their cybersecurity posture.

1. Describe your organization and its interest in the Framework.

Cybernance has developed software that helps corporate boards and executive leadership understand their organization's cyber risks. Our software is used as both a diagnostic for gauging cyber risk management maturity, and as an engine for recommending and prioritizing specific mitigation efforts. The NIST Framework serves as the backbone of the software's evaluation and recommendation architecture.

2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

In my role as a product manager for Cybernance, I am both a user of the framework, and a SME. I represent one organization (Cybernance) whose mission is to deploy the NIST Framework into multiple organizations.

3. If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).

First and foremost, Cybernance used the Framework as a basis to develop our software, the Cybergovernance Maturity Oversight Model (CMOM). CMOM is a blend of two frameworks: 1) informed by the CSF Implementation Tiers, and 2) aligned with the Dept. of Energy's C2M2. CMOM delivers an assessment of enterprise security maturity that is scored against C2M2 using the Implementation Tiers put forth in the CSF. We use this software to assess our own security and the security of our customers.

4. What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?

Each of the components of the CSF is important in understanding the whole. The Core is a tremendously useful guide for conversations about what cybersecurity means. The component most prominently featured in our software is the Implementation Tiers. We found these to be much more meaningful and intuitive than the C2M2 "Maturity Indicator Level" (MIL). We also adapted the Implementation Tiers to apply at a more granular level. In our CMOM security evaluation software, each individual security control is described at Implementation Tiers 0-4. This gives the user a set of prompted responses that are descriptive at a meaningful level of detail, which increases the accuracy and value of their responses.

5. What portions of the Framework are most useful?

Implementation Tiers and the Core. Separately and together, these are highly intuitive descriptions of security practices, and are useful for bringing non-technical stakeholders into the conversation.

6. What portions of the Framework are least useful?

Profile. The intent of the Profile is understood, but the presentation isn't as fully developed as the other components of the CSF. For the Profile to be useful, it would need guidelines and parameters that will enable non-technical stakeholders to adapt the tool to their organizations. Its current form provides a high-level recommendation without guidance about how to achieve that recommendation.

7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?

Not quite a limitation, but an occasional hurdle arises when we encounter a customer who relies on ISO, COBIT, or some other framework. Our response has been to embrace their successes with these frameworks, and then show how the CSF incorporates best practices without being prescriptive, allowing the Framework to adapt to any organization. If there were official studies or statements that support this viewpoint, those would be very helpful to have.

8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.

We formed our company (February 2015) around the principles of the CSF, so we were fortunate not to have legacy systems or residual risk to deal with. That said, the Framework has informed our relationship with partners and customers, and helped significantly reduce the third-party risk that many of us are familiar with from previous ventures.

9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?

No comments for #9.

10.Should the Framework be updated? Why or why not?

The Framework should aspire to the highest Implementation Tier – to be adaptive. This RFI is an excellent way to enable those adaptations; by seeking field experiences and evaluating them in aggregate for trends. The CSF should avoid becoming prescriptive or technology-focused. It should be built around first principles, and leave specific implementations to the user.

11.What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

The Profile section could use significant development. Compared to the Core and the Implementation, it doesn't provide nearly as much guidance as we would expect. Our business addresses the gaps between board- and executive-level managers and their operations-level security teams when it comes to understanding cybersecurity. Often, illuminating the problems (of which there are many) simply leads to paralysis; management isn't sufficiently capable of understanding what to do next, so they default to inaction. The Profile should enable this action in the same way that the Core and Implementation Tiers have illuminated shortcomings. This is what the CMOM software aims to do.

12.Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

Refer to comments in #11.

13.Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?

No comments for #13.

14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?

Our customers consistently demonstrate acute needs in two areas of cyber risk management: 1) supply chain/third party risk, and 2) risk valuation methods. Each of these practice areas has precedent in older applications (non-cyber risk) and could be informed by attention to first principles. We are optimistic that further attention to data analysis will begin to reveal patterns that can be associated with best practices for risk management. In the Roadmap, NIST discusses the potential of cyber data to inform our progress. Cybernance would be an active participant in such studies.

15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

Ensure that any updates include appendices with clear and complete notation of changes, additions, and subtractions.

16. Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

We use the NIST SP series as supplemental materials in our software documentation. Customers who seek guidance on next steps – once security gaps have been identified – are referred to the appropriate SP.

17. What, if anything, is inhibiting the sharing of best practices?

Best practices would be more easily shared if they could be done so via measureable standards. This includes not just implementation levels, but also the cost – in time and dollars – of those implementations, ongoing maintenance requirements, and measures of the value that was provided. Of course, this is far more easily said than done. We anticipate that the ongoing use of data analysis methods will begin to reveal measurements that can inform standards.

18. What steps could the U.S. government take to increase sharing of best practices?

No comments for #18.

19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

No comments for #19.

20. What should be the private sector's involvement in the future governance of the Framework?

Private sector should be invited to participate through public comment forums, information sharing, case analysis, and data analytics. Stakeholders should be eligible for roles overseeing the collection, aggregation, and analysis of information, so that private sector experiences can be integrated into the methods by which the framework is developed. Governance should remain in the hands of NIST.

21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

We believe the Framework should strive to be a Standard – which implies that its custodian should remain NIST. Whoever oversees the CSF, their mission, goals, and vision should be technology agnostic to avoid the CSF turning into a prescriptive checklist.

22. If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?

Refer to comments in #21.

23. If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?

Refer to comments in #21.

24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

Refer to comments in #21.

25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

Refer to comments in #21.